JSOU

# Information Warfare: Assuring Digital Intelligence Collection

William G. Perry

JSOU Paper 09-1
July 2009

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **JUL 2009** | | **00-00-2009 to 00-00-2009** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Information Warfare: Assuring Digital Intelligence Collection** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Special Operations University,357 Tully Street Alison Building,Hurlburt Field,FL,32544** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | **Same as Report (SAR)** | **48** | |


## Joint Special Operations University and the Strategic Studies Department

The Joint Special Operations University (JSOU) provides its publications to contribute toward expanding the body of knowledge about joint special operations. JSOU publications advance the insights and recommendations of national security professionals and the Special Operations Forces (SOF) students and leaders for consideration by the SOF community and defense leadership.

JSOU is the educational component of the United States Special Operations Command (USSOCOM), MacDill Air Force Base, Florida. The JSOU mission is to educate SOF executive, senior, and intermediate leaders and selected other national and international security decision makers, both military and civilian, through teaching, outreach, and research in the science and art of joint special operations. JSOU provides education to the men and women of SOF and to those who enable the SOF mission in a joint and interagency environment.

JSOU conducts research through its Strategic Studies Department where effort centers upon the USSOCOM mission and the commander's priorities.

**Mission.** Provide fully capable special operations forces to defend the United States and its interests. Plan and synchronize operations against terrorist networks.

**Priorities.**
- Deter, disrupt, and defeat terrorist threats.
- Develop and support our people and their families.
- Sustain and modernize the force.

The Strategic Studies Department also provides teaching and curriculum support to Professional Military Education institutions—the staff colleges and war colleges. It advances SOF strategic influence by its interaction in academic, interagency, and United States military communities.

The JSOU portal is https://jsoupublic.socom.mil.

**On the cover.** U.S. Army soldier collects sensitive materials, including a computer hard drive, following the arrest of an Iraqi man for involvement with the manufacture of improvised explosive devices in the city of Dora in southern Baghdad, Iraq, 13 August 2007. (U.S. Air Force photo by MSgt Jonathan Doti.)


# *Information Warfare: Assuring Digital Intelligence Collection*

William G. Perry

**JSOU Paper 09-1**
*The JSOU Press*
*Hurlburt Field, Florida*
*2009*

The JSOU Strategic Studies Department is currently accepting written works relevant to special operations for potential publication. For more information please contact Mr. Jim Anderson, JSOU Director of Research, at 850-884-1569, DSN 579-1569, james.d.anderson@hurlburt.af.mil. Thank you for your interest in the JSOU Press.

*******



ISBN 1-933749-37-7

*Recent Publications of the JSOU Press*

**Psychological Operations: Learning Is Not a Defense Science Project,** March 2007, Curtis D. Boyd

**2007 JSOU and NDIA SO/LIC Division Essays,** April 2007

**Hunting Leadership Targets in Counterinsurgency and Counterterrorist Operations,** June 2007, Graham H. Turbiville, Jr.

**Executive Report, JSOU Second Annual Symposium** (30 April–3 May 2007)

**A Theory of Special Operations,** October 2007, Robert G. Spulak, Jr.

**Block by Block: Civic Action in the Battle of Baghdad,** November 2007, Adrian T. Bogart III

**Private Security Infrastructure Abroad,** November 2007, Graham H. Turbiville, Jr.

**Intelligence in Denied Areas,** December 2007, Russell D. Howard

**Is Leaving the Middle East a Viable Option,** January 2008, Thomas H. Henriksen

**Retaining a Precarious Value as Special Operations Go Mainstream,** February 2008, Jessica Glicken Turnley

**Disrupting Threat Finances,** April 2008, Wesley J.L. Anderson

**USSOCOM Research Topics 2009**

**India's Northeast: The Frontier in Ferment,** September 2008, Prakash Singh

**What Really Happened in Northern Ireland's Counterinsurgency,** October 2008, Thomas H. Henriksen

**Guerrilla Counterintelligence: Insurgent Approaches to Neutralizing Adversary Intelligence Operations,** January 2009, Graham H. Turbiville, Jr.

**Policing and Law Enforcement in COIN—the Thick Blue Line,** February 2009, Joseph D. Celeski

**Contemporary Security Challenges: Irregular Warfare and Indirect Approaches,** February 2009, Richard D. Newton, Travis L. Homiak, Kelly H. Smith, Isaac J. Peltier, and D. Jonathan White

**Special Operations Forces Interagency Counterterrorism Reference Manual,** March 2009

**The Arabian Gulf and Security Policy: The Past as Present, the Present as Future,** April 2009, Roby C. Barrett

**Africa: Irregular Warfare on the Dark Continent,** May 2009, John B. Alexander

**USSOCOM Research Topics 2010**

# Foreword

The advent of the digital age has made it inevitable that troops in contact will fall upon computers and related equipment valuable for the information they can provide about the enemy. In this paper, Dr. William G. Perry provides some guidelines about processing computer equipment for transfer to information and intelligence professionals who might wring out from digital storage media the critical information needed to penetrate the enemy's decision matrix. In addition, captured computer gear may often need to be protected by a chain of custody in order to support legal actions against illegal combatants—criminals.

The digital age meshes with the 21st century irregular warfare environment in which nonstate actors, armed groups, terrorists, and criminals confront established governments. Today's Special Operations Forces (SOF) are most likely to confront these opponents while on counterinsurgency, foreign internal defense, and counterterrorism missions. From the moment of tactical discovery until its presentation in the courtroom, digital evidence will need to be safeguarded and a valid chain of custody maintained so that the host nation (or U.S. Government) might successfully bring criminals to justice. This will fall on the shoulders of the SOF operators at the tip of the spear who must add yet another skill set to their already full rucksacks.

Particularly in direct action missions, the need to properly capture and bag-up enemy digital material can be critical to mission success, both for intelligence and legal purposes. Every strike team that descends upon the target will consider employing a "forensics team" that can rapidly identify sources of valuable digital information, document the findings, and secure computers and storage media.

While conducting actions on the objective, it may seem a bit too much to expect a SOF team to devote effort to fiddling with such details. Dr. Perry stresses that mission accomplishment and security will always be first in the minds of the warfighter, but the digital forensics effort will produce important results. The legitimacy of host-nation governments, and indeed the U.S. Government, is reinforced many fold when military operations are founded on the rule of law. Dr. Perry's ideas for "Assuring Digital Intelligence Collection" are tactical techniques that have a significant strategic payoff.

James D. Anderson, Director of Research
JSOU Strategic Studies Department

# About the Author

Dr. Bill Perry is director of the Center for Information Technology and Assurance in the College of Business at Western Carolina University. He is a professor of computer information systems and teaches computer networking and information security. He also serves as a member of the Academic Council of the Center for Security Policy and is an associate fellow with the JSOU Strategic Studies Department.

Dr. Perry is the author of *Developing Professional Information Security Competencies*. He received the Global Teaching Excellence Award and was twice awarded the Board of Governor's Innovative Teaching Award from the University of North Carolina system. He recently won the Proteus Monograph Competition at the U.S. Army War College with a topic that focuses upon exploiting open source information.

A former U.S. Navy officer, Dr. Perry also has experience in counterintelligence and threat assessment. He has presented at national conferences on the topic of information warfare and has coordinated and participated in various security-related workshops involving the Federal Bureau of Investigation, Central Intelligence Agency, and U.S. State Department. Dr. Perry also served as editor on two books related to the intelligence community and has made national presentations on protecting critical infrastructure.

A student of Russian and Chinese information warfare, Dr. Perry completed the National Security Agency's course, Information Security Assessment Methodology. He is a founding member of a new IEEE Technical Committee on Information Assurance and Intelligent Multimedia-Mobile Communications and also provided input in establishing the technical committee's initial objectives.

Dr. Perry received his B.A. in Business Education from the University of South Florida. He went on to receive his M.A. and Ph.D. in Business Education from the University of North Dakota. He presently lives in Cullowhee, North Carolina.

# Introduction

> *The military establishment must acknowledge that the face of battle is changing. Information, as a dimension of conflict and competition, has vaulted to the forefront of importance of the future national security landscape and now must rank as at least co-equal with air, ground, sea, and space dimensions. Yet, even with its importance, we have just begun the intellectual examinations necessary to develop a viable theory of IO [information operations] that will underpin any discussion of war in the digital age.*[1]

Information warfare may be as old as mankind, but the methods and the means of its application today are totally new. Key tactical information can be contained on digital storage devices that are worn on the body like jewelry. The enemy can transmit information with deadly results from devices that remain unseen to all but the trained eyes of those who know how to discover, secure, and preserve digital intelligence.

Code books, maps, encryption devices, and paper documents were once the subject of searches for useful intelligence on the battlefield. We still search for similar information, but critical data today can be found on a secondary storage media that is the size of a fingernail, in electronic address books and cell phone memory, or written in unseen logs of data packets that have streamed into and out of the enemy's Internet-connected computer.

Discovering and preserving the enemy's critical electronic data can be game changers. We can gain a competitive advantage by being astute and co-opting the enemy's digital intelligence. We can glean electronic intelligence and get inside our adversary's decision-making loop.

The armed forces of the enemy, terrorists and criminals, use computers the way we do—for command and control purposes, to store information on personnel, to send and receive e-mails and text messages, to encrypt files, and to implement codes. High value information specifying size of force, battle logs, and plans for future action has all been discovered on seized electronic equipment. Files and disks, CDs, and DVDs that contain time and date stamps, Internet traffic logs, and data on the movement and whereabouts on an adversary's assets can all be recovered. Vital information can also be gleaned from unlikely electronic devices, such as digital picture frames, MP3 and MP4 players, and a variety of novelty storage media. The

enemy is smart about how computers can be used as instruments of war and is getting smarter. We must do the same.

The likelihood that Special Operations Forces (SOF) will encounter computers, portable electronic equipment (e.g., personal data assistants, cell phones, and gaming systems) and digital storage media is high. The big challenge for SOF is to recognize, secure, and safeguard as much of the discovered data or information as possible so that it can be subjected to forensic analysis. Successfully discovering, preserving, and assuring digital intelligence for exploitation and legal purposes is essential to support our country's national security objectives against those who would do harm.

SOF are likely to be in the first-responder role for digital information. The data that is stored on electronic devices can easily be damaged if mishandled. Digital data is at risk of being destroyed, modified, or lost due to the volatile nature of electromagnetic storage and other technical issues. Alteration or damage to a few bits (i.e., 1s and 0s) of data can render much of what is stored on a memory device as useless.[2] See Appendix A to learn more about the nature of stored information.

Corrupted data may be impossible to recover for analysis. Further, computer (or digital) based evidence may be worthless unless it is collected and presented in court in such a way that it will not contravene the rules of admissibility and will lead to the successful conviction of criminals (or terrorists).[3]

Seizing electronic devices and obtaining digital data fall under rules for information operations as promulgated by the Department of Defense. See Appendix B for a perspective of the Joint Chiefs on information operations. All branches of the armed forces are obliged to follow multinational doctrine and procedures that are consistent with U.S. law, regulations, and doctrine.

The purpose of this monograph is to help operators discover, preserve, and assure information assets so that they can be exploited for intelligence and legal purposes.

# Statement of Problem

The challenge addressed in this monograph is to develop an understanding of how SOF can conduct IO (from tactical entry, discovery of digital assets, and the establishment of a valid chain of custody) without unnecessarily endangering the lives of operators while still assuring the integrity of digital information.

The task for operators is to follow procedures and protocols for data discovery and seizure that assure the preservation of highly volatile and perishable digital information. Stored digital information is very fragile. The precise manner in which electronic media is physically handled and collected from the target *can* place the integrity of stored digital information at risk. Data can be easily damaged, destroyed, or inadvertently modified.

The basics of assuring the integrity and usability of digital information must be employed to ensure the value of the digital information. Circumstances in the field, however, can rapidly become chaotic and unpredictable. The safety of operators is first. Electronic evidence, however, remains among the most problematic to assure.

SOF team members need to be able to identify potential sources of electronic information; recognize computers, network components, and storage media; and apply essential information assurance techniques.

## SIDS: Digital Search and Seizure Procedures

A number of rational and well-conceived principles can be used to guide operators when involved in the search and seizure for digital information and electronic devices. Operators can remember the essence of the procedures with the acronym, SIDS, which stands for scan, identify, document, and secure.

Table 1. Basic Search and Seizure Principles for Electronic Information

| Step | Description |
|---|---|
| Scan | 1. Visually scan the environment for the presence of electronic media and devices.<br>2. Scan the area for the presence of a wireless network. |
| Identify | 3. Identify electronic devices, all digital devices, media, and connections.<br>4. Identify any network connections (local or external).<br>5. Examine the devices for any visible damage. |

Table 1. Basic Search and Seizure Principles for Electronic Information (cont'd)

| Step | Description |
|---|---|
| Document | 6. One team member (wearing an antistatic wrist band), if possible, should be responsible for custodianship and logging electronic devices.<br>7. Log any visible physical damage.<br>8. Photographically document room(s) in which the equipment is found, the front and back of the computer, and/or sketch any physical evidence (including cords and connections) to be seized before removing.[4]<br>9. Determine if device is on or off; it is *on* if the screen has content. Otherwise, look for lights or sounds.<br>10. Operators should avoid interacting with the computer in any way, unless so ordered (i.e., on-loading surveillance software may actually be the mission).<br>11. Secure the storage and electronic devices for removal using labels (to include the collector's initials, date, and time), putting evidence tape on the back of the machine, and store seized equipment in antistatic plastic wrap or bags (i.e., cardboard boxes and cotton cloth can be used as an improvised substitute).<br>12. Record all activities conducted and maintain a chain of custody; see Appendix C. |
| Secure | 13. Secure any printed material or hard-copy evidence.<br>14. Power down any devices that are on and log the time of the shut down.<br>15. Safely secure seized electronic devices and media for transport in any hard-shell case (if available), cardboard box, packing foam, antistatic plastic wrap, or cotton cloth.<br>16. List what is contained in each container that is being transported when time permits and seal with evidence tape. |

**What types of electronic media and devices should be considered when scanning the environment?** Operators should scan the environment for a variety of computers and electronic devices that are capable of storing information. Computers include desktops, laptops, notebooks, and sophisticated hand-held devices such as iPhones and iTouch devices and a Blackberry. Images of a number of these devices are shown in Figure 1.

Other electronic devices can be used to store digital data. Operators should be able to identify them. Table 2 lists a number of digital devices that can be used to store data.

Even a Microsoft Xbox can be turned into a Linux network server capable of supporting an entire network of computers. Other devices that can process and store information include TiVo, DVD players, and any number of personal entertainment equipment.[5]

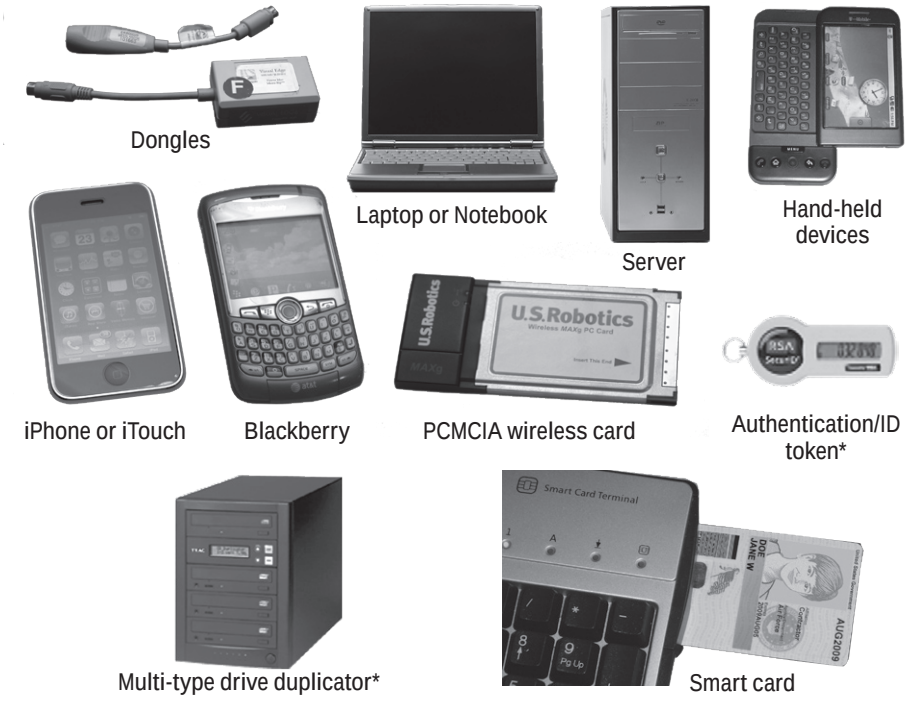



Figure 1. Examples of Electronic Media and Devices
(*courtesy Dell Computers)

Table 2. Other Electronic Devices Can Contain Digital Data

| | | | |
|---|---|---|---|
| • Answering machines | • Audio recorders | • Caller ID devices | • Cellular telephones |
| • Chips | • Copying machines | • Databank/organizers | • Digital cameras (still and video) |
| • Digital picture frames | • Disks, CDs, & USB drives | • External hard drives | • Fax machines |
| • Flash memory cards | • GPS devices | • Pagers | • Personal data assistants |
| • Printers | • Removable media | • Scanners | • Telephones |
| • Video recorders | • Wireless access points | • Video game consoles and media | |

**What type of media can be used to store electronic information?** Operators should look for the presence of typical computer storage media; Figure 2 provides examples.

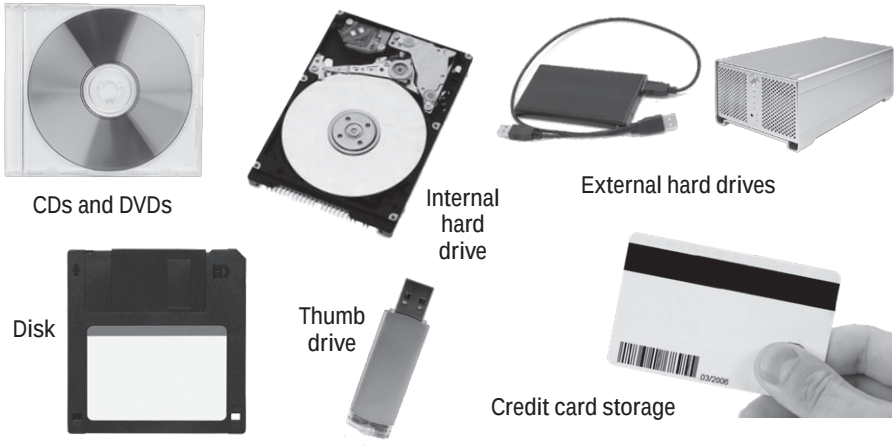



Figure 2. Typical Computer Storage Media

The design of some storage devices falls into the category of being novelty storage media and may be deliberately deceptive. Examples include USB wrist bands as well as the deceptive Swiss army knife and pen USB drives shown in Figure 3.

Figure 3. Pen USB drive and Swiss Army knife with USB

Other storage media is so small that it can easily be overlooked lying on any surface. One such medium is known as SD (Secure Digital) disk memory. A significant amount of information can be stored on an SD, and it can be as small as a postage stamp or fingernail. Some examples displayed in Figure 4. Operators should be on the lookout for any gadget, mechanism, or apparatus that can be used to store electronic content.

Figure 4. SD Disk Memory

**How do you recognize a computer network when scanning the environment?** Computers can communicate with other computers when they are connected. The connection can either be wired or wireless. Operators can recognize a computer that is capable of communicating with a network in two ways.

The first way to determine if a computer is on a network is to look at the connections on its back. If more than a power cord is hanging off of the back of the computer, it is connected to something. A computer that is *hard-wired* to an internal network or the Internet uses a NIC (network interface card). The connection is either made using an RJ45 connector, coaxial cable, or what may appear to look like a cell phone or satellite radio. The wire or cable coming off the back of the computer is either connected to a router or what might appear to be an outlet on the wall.

If the computer is connected to a router, it can be hard-wired to other computers or be broadcasting to other computers wirelessly. Figure 5 shows examples of computer networking media and devices.

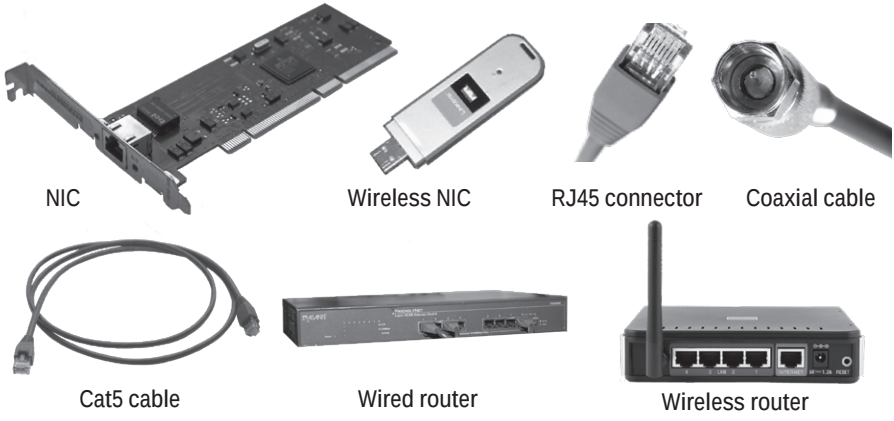



Figure 5. Examples of Computer Networking Media and Devices

A NIC can be manually inserted into a vacant slot on the inside of the computer or built-in on the motherboard. The operator must determine what device the computer is connected to if more than a power cord is connected to the back of the computer. Devices that are identified must also be seized if at all possible. Regardless, a *wireless* network may still be present.

Operators need to establish whether there is evidence of a wireless network. The area can be quickly scanned using a wireless signal detection device (like the ones shown in Figure 6).


Figure 6. Wireless Detection Devices (* courtesy SPY Associates, www.spyassociates.com; ** courtesy Dell Computers)

Certain cell phones, an iPhone, or other personal hand-held communications equipment can alternatively be used to detect the presence of a wireless network but might be less helpful in detecting the exact location of other computers and devices.

Discovering a wireless network can result in a major payoff because the distance that a wireless signal can travel is limited (under 300 feet). The presence of a wireless network indicates that other computers and hardware are close and need to be secured if time permits. A large capacity wireless hard drive, for example, might be hidden from view and mounted in the ceiling or behind a wall. Figure 7 shows a wireless storage device.

Figure 7. Wireless Hard Drive (courtesy Dell Computers)

**What should happen after successfully scanning the environment and identifying computer hardware and network components?** Enemy computers or electronic components, once discovered and identified, must be thoroughly documented and secured for safe transport. The original state of the electronic devices must be photographed or sketched and only limited interaction with the equipment, components, and storage media should occur. Operators should avoid exceeding their knowledge level with regards to electronic equipment. Successfully preserving digital intelligence

for forensic analysis will allow intelligence analysts the opportunity to step "inside" the adversary's decision-making cycle. See Appendix D on computer forensics.

**How do you document the scene and what is seized?** Photograph and/or sketch the actual physical space in which electronic devices or media is discovered, if possible, as soon as the space is secured. The images on the monitor of any computers that are turned *on* must be photographed. The layout and contents of the room(s) should also be documented with photos or sketches.

Pictures should be taken of the front, back, and sides of all computers and devices that are discovered before being touched or moved. All connections should also be documented. Evidence tape, ideally, should be placed on any open computer drive bays and other access points on the computer case, including the opening for the power plug when it is eventually unplugged.

A voice-activated audio recorder would likely be the best alternative for documenting or logging activities when safety and time are critical.

A number of possible scenarios exist that operators might encounter, thus they will be explored in this monograph. Following procedures that increase the chances of successful information preservation become very important.

**Every situation is different. How should you react?** SOF may discover computers, unexpected electronic devices (e.g., MP3 players, personal data assistants, cell phones, land-line telephones, voice recorders, answering machines, computers, fax machines, copying devices, and paging devices), and media in the course of carrying out mission objectives. Digital cameras, DVD players, and home entertainment devices also have large storage capacity that the enemy can use to store a significant amount of information. Critical information and data (intelligence) can be discovered when very little is expected (e.g., phone numbers stored in memory, PINs, passwords, or messages).

Use the general SIDS procedures if time and safety permit. The environment should be scanned to identify electronic devices, computer networks, and storage media as soon as possible. Prevent all interaction with computers or electronic devices at the scene. One individual, if possible, should process any electronic devices that are discovered. That which is

discovered for seizure should be photographically documented or sketched. An evidence log should be initiated when it is possible to do so without endangering personnel.

Electronic devices, cords, cables, and connectors should be labeled for each unique device and secured for safe transport. An effort should be made to take the computer mouse because it is capable of storing large amounts of data. Pens, watches, cassette tapes, and even a Swiss army knife can potentially hold memory cards or larges amounts of stored information.[6] All manuals or other printed materials related to the electronic devices should also be seized.

In all likelihood a need would exist to transport or remove the computer or media from the scene. Devices should be packaged in antistatic material, when possible, and put in a case that is designed to transport fragile items. Any electronic devices or storage media must be kept away from magnets, moisture, dirt, dust, radio signals, or other high energy electromagnetic fields (including electric motors).

When conducting highly dangerous combat operations, maintaining a well-documented chain of custody is near the bottom of the list of priorities. Establishing a chain of custody that might be used in later legal proceedings, however, moves closer to the front of the line once the safety of team members has been assured.

The assumption is made that the computers or electronic devices discovered on the scene must be quickly removed. Otherwise, if time permits, there would be other forensic techniques that must be applied (i.e., a RAM dump and/or the copying of files, imaging the hard drive, recording processes that are running, observing services that are presently being run, searching for IP addresses and possibly noting permissions to other off-site resources).

What follows are a number of scenarios that indicate what can be done if enemy computers, electronic devices, or storage media are discovered.

## Scenario 1. Computer or electronic device is discovered in a power-*on* condition.

When a desktop computer or electronic device is discovered in a powered-up condition, the computer should be left *on* until basic documentation has occurred. The contents of the screen should be photographed.

Operators should immediately restrict the number of people who come into contact with the digital device. Any digital devices must be secured and prevented from coming into contact with any other electronic devices. The complete scene should be photographically documented or sketched. Any visible connections on the computer should also be documented.

The room or area should be checked to determine if any wireless telecommunication signals are present. The possibility exists that other devices may be operating wirelessly and connected to other computers like a wireless electronic storage device. If a wireless signal is found, a quick search of the area (i.e., in the ceiling, behind walls) should be performed if time permits.

Remaining steps to keep in mind follow:

a. Power down the computer after documenting the device by pulling the plug from the wall or the power supply.
b. If possible, place evidence tape on all drive bays or any openings on the devices that are discovered. If time permits, attach labels to each connection that is visible.
c. Begin an evidence log as soon as the operation is secured and team safety is assured.

## Scenario 2. Single computer or electronic device is discovered in a power-*off* condition.

Upon discovering a computer or electronic device and determining that it is turned *off*, do *not* turn on.[7] Examine the connections on the back of the computer and photograph them. Label any connections so as to assist in reassembly. Take pictures of the computer and any other devices to which it is connected.

Other areas for attention follow:

a. Unplug the computer from the wall (if plugged in) and remove any connection from the back of the computer that appears to be connected to a telephone or other device. Computers can be turned on remotely, and all relevant evidence could be erased.
b. Check the room or area for the presence of wireless signals. Identify, document, and secure any wireless devices that are discovered.

c. Take pictures of electronic devices and media before touching them. Place evidence tape, if time permits, on all drive bays and open receptacles on any computers, media, and other devices that are discovered. Take special care when transporting the machine and keep the device(s) away from high energy fields such as magnets and radio transmitters.

## Scenario 3. Monitor of a desktop computer is *off,* but the computer is *on*.

Attempt to determine if the discovered computer is in a power-*on* condition or running. The CPU might be running with the monitor off. Listen carefully for any electronic noises, possibly from a fan motor or storage mechanism. Look for any lights on the computer. Here are the corresponding actions:

a. Turn on the monitor and document the contents that appear on the screen.
b. Scan the area for the presence of any wireless signals. Identify, document, and secure any wireless electronic devices that are discovered.
c. Take pictures and label any connections on the back of the computer or electronic devices that are found. Also document any changes made to any discoveries.
d. Remove any devices from their power sources by unplugging them from the wall. Secure the computer for safe transport in antistatic bags and keep the device away from high energy fields or extreme conditions.

## Scenario 4. Stand-alone computer is discovered.

Photograph the screen and all connections if the device is powered up. *Note:* Do *not* turn on the computer or device if it is powered down. Two other actions follow:

a. Check the area for any wireless signals. Identify, document, and secure any wireless computers or devices that are discovered.

b. Document and label all connections on all devices. Place evidence tape on all openings of the computer case. Secure the devices for transport and establish the chain of custody.

## Scenario 5. Portable computer is discovered.

Upon discovering a portable computer (e.g., notebook or laptop), check to determine if it is connected to either a power source or other device. Avoid turning the computer *on* if it is *off*. Also scan the environment to determine if there are any wireless signals being broadcast. Related thoughts or remaining actions follow:

a. If the power is *on* when the portable computer is discovered, photograph the screen as well as the back and all connections. Avoid turning *off* the power of the portable computer if at all possible by keeping the battery charged. Be sure to document any changes made in the computer from the way it was found (e.g., plugging a laptop into a recharger).
b. Check to determine whether the portable computer is in what is known as a *low power mode*. The screen can be blank and even the lid closed. Double check to see if a faint LED light is blinking on the front of a portable computer. That would indicate that the laptop is in a low power mode. If a portable computer is discovered in a low power mode, follow the steps in Scenario 1.
c. If not in a low power mode, perform a hard-power down—that is, hold down the power switch for at least 10 seconds. Attach evidence tape to the case and any openings on the back.
d. The on-scene operators should also attempt to locate any carrying case for the portable computer and document its removal from the premises. The case and its contents (i.e., extra USB drives or disks, CDs, or DVDs) could contain significant information.
e. Secure the computer for safe transport.

## Scenario 6. Networked computers and peripheral devices are discovered.

Check the back of a computer to determine if it is connected to a network interface card via an RJ45 connector. Scan the environment for a wireless

signal. Discovering computers and other devices that are connected are very significant. At least one or more workstations are connected to a network server. Finding a network server could provide a gold mine of useful intelligence. The likelihood of a server also being connected to the Internet is high.

Pictures should be taken of any monitors that are powered up, and any connections between the electronic devices should be documented and labeled. Evidence tape should be placed on all the drive openings on the computer, router, devices, or media for safe transport.

## Scenario 7. External storage devices and media are discovered.

External storage devices may include disks, CDs, DVDs, USB drives, cell phones, personal data assistants, compact flash drives, MP3 players, cassettes, electronic games, or other devices (i.e., a digital picture frame). An effort to discover these devices should be made and documented in the location where they are discovered, then label and apply evidence tape. Ideally, only one individual should handle the device. Other actions follow:

a. Any external devices that are plugged into a power source should be examined. If any lights are on or showing, pictures should be taken of the front of the device.
b. Any connections to the back of the device should also be noted. The connections should be labeled and disconnected from the power source.
c. Any devices that are discovered should be placed in an antistatic wrapping and securely packaged for transport.

## Summary

SOF are called upon to conduct direct action missions that support the national security objectives of the United States. Increasingly, SOF operates in an asymmetric threat environment in which electronic devices and storage media are used directly by the enemy to support their ability to conduct war. SOF are likely to encounter computers and electronic equipment when conducting operations. The opposition continues to expand its use of electronic information, and the U.S. needs to counter the threat by conducting effective and intelligent information operations.

Electronic devices and information that are stored in computer memory or other media can be extremely volatile and can easily be destroyed or modified. This fact is true even under normal operating conditions.

The discovery of electronic information and devices can either be *expected* or *unexpected*. A good chance exists that actionable intelligence can be gleaned from seized electronic devices by following digital assurance best practices. Establishing a chain of custody can also increase the chance that terrorist action can be thwarted and successfully prosecuted.

# Glossary

| | |
|---|---|
| binary | Technique for representing data as a series of 1s and 0s |
| CPU (central processing unit) | Portion of the computer where high speed computations occur |
| computer forensics | Application of computer investigation and analysis techniques to determine potential legal evidence (or intelligence)[8] |
| data | Representation of facts that can be used for processing and creating information for decision making |
| digital evidence | Information that is stored in electronic format using the binary numbering system |
| dongle | A device that plugs into available computer port (i.e., USB) and performs a useful service such as encryption, infrared data transfer, or network connectivity) |
| hardware | Any object or component that can be associated with a computer system |
| information | Processed data |
| information assurance | Methods and techniques used to assure the confidentiality, legacy, integrity, and nonrepudiation of information |
| information operations (IO) | Integrated employment of the core capabilities of electronic warfare, computer network operations, psychological, deception, and operations security in concert with specified supporting and related capabilities to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own |
| Internet | Network(s) that connects millions of computers across the globe using internationally accepted protocols |
| IP (Internet Protocol) | The standard that works with Transmission Control Protocol (TCP)—that is, describes how an Internet-connected computer should break data down into packets for transmission across the network, and how these packets should be addressed, so they arrive at their destination[9] |
| Linux | Computer operating system |
| media | Computer storage mechanisms (e.g., hard drives, USB drives, disks) as well as the means of transmitting data (i.e., twisted wire pairs, fiber optic) |
| network | More than one connected computer |
| protocols | Standardized rules for electronic communications |
| RAM (Random Access Memory) | Volatile electronic storage that retains data only as long as power is being received |
| RAM dump | Copy of volatile memory that can include unsaved documents, chat sessions or text messages, passwords, and other critical information |
| RJ45 | Computer network connector |
| ROM (Read-only Memory | Memory that is permanently inscribed on a computer chip |
| server | Computer that manages network resources and authorized users |

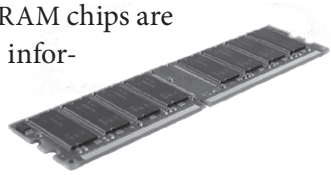
| | |
|---|---|
| TCP/IP | The complete Internet protocol suite—that is, set of protocols for transmitting data over computer networks and the Internet |
| uninterrupted power supply | Usually a short-term emergency backup power supply for a computer or electronic device |
| volatile | Fragile or subject to easy destruction |
| wireless | Term frequently used to describe a computer network connection that is accomplished without a physical connection |
| wireless hard drive | External storage device, which likely contains a massive storage capacity that can connect to a computer or networks *wirelessly*; wireless storage devices can connect to routers using radio frequency (RF) technology and be easily hidden from view (i.e., above ceiling tiles or behind walls) |

# Appendix A. The Nature of Stored Information

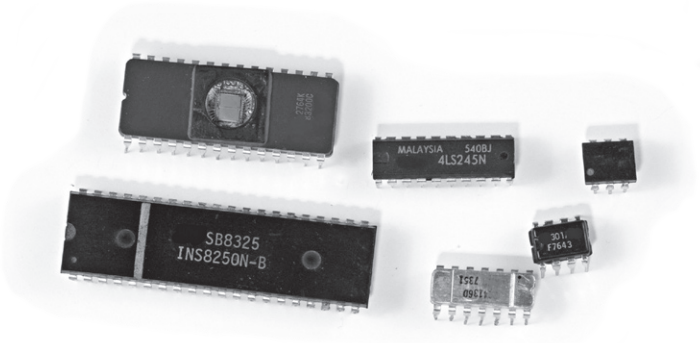
Electronic data consists of charges that are either processed or recorded on magnetic media. A single *positive* charge may be thought of as a "1" and a *negative* charge as a "0." Alphabetic characters, numbers, and specialized symbols are represented by a fixed series of 1s and 0s that can be reviewed in the ASCII table (as shown in Appendix E).

Data is processed and turned into information.

Electronic data can be permanently or temporarily stored on chips in computer memory or on secondary storage devices (commonly referred to as CDs, DVDs, or disks). Random Access Memory or RAM (usually located inside the device) stores information that is volatile. RAM retain data only as long as it is receiving power. RAM is volatile and usually connected to the internal motherboard of the computer. If RAM chips are found loose or unattached, secure them. Useful information about the nature of the enemy's devices and systems could be gleaned. An examples of a RAM chip is displayed on the right.



The second type of internal memory is known as Read-only Memory or ROM. The instructions contained on a ROM chip are executed when the device is powered *on*. ROM chips are usually found inside the computer. Any ROM chips found loose should also be secured for their intelligence value. Shown below are images of ROM chips.



Both user-created and computer-generated information can be potential sources of useful information, but operators must remember that electronically stored media is extremely delicate. Some data that is electronically stored is volatile (it would disappear if the power was turned off) whether it is being processed, transmitted, or stored. Turn off the power, and the data disappears.

Exposure to a powerful magnetic field, for example, can erase or alter stored information. Exposure to vibrations, shocks, moisture, or rough handling can cause stored information to be lost.

The basic characteristics of electronic information must be understood; a summary follows:

a. *Storage media* includes hard drives, CDs, DVDs, disks, SD disks or flash memory, USB drives, external hard drives, network storage devices, and wireless storage devices. Data stored on media are all forms of *secondary storage*.
b. Information that is stored in RAM or ROM is referred to as *primary storag*e or *memory*.
c. Preserving the usefulness of digitally stored data involves the careful collection and documentation of electronic media. For example, data that is recorded on secondary storage and exposed to magnetic or electromagnetic fields can be altered or destroyed and lost forever.

# Appendix B. Information Operations: The Joint Chiefs of Staff Perspective

Senior military officials view information as being a "strategic resource, vital to national security, and [that] military operations depend on information and information systems for many simultaneous and integrated activities."[10] *Information operations* is defined as any actions taken to affect the adversary's information, information systems, and decision making while defending one's information, information systems, and decision-making capability. Information operations include many dimensions such as electronic warfare, computer network operations, psychological operations, military deception, and operations security.

SOF contribute directly to information operations "in concert with specified supporting and related capabilities to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."[11] Successful planning, preparation, execution, and assessment of information operations (IO) demand detailed and timely intelligence, and this must be conducted in a manner that positively affects net intelligence gains or losses.

One of the most important perspectives of the Joint Chiefs is summarized in the following quote: "The IC (Intelligence Community) must implement technical and procedural methods to ensure compliance with the law," and that "specific sources and methods be positioned and employed over time to collect the necessary information and conduct the required analyses."[12]

Part of the joint mission objectives of Special Forces and IO is following methods and techniques that legally assure digital information for forensic purposes. The services, United States Special Operations Command, and federal agencies develop capabilities based upon their core competencies embodied in law, policy, and lessons learned. Joint Publication 3-13 emphasizes that IO can affect data, information, and knowledge "by taking actions to affect the infrastructure that collects, communicates, processes, and/or stores information in support of targeted decision makers."[13]

Included in the most recent IO doctrine established by the Joint Chiefs is a recognition that information is a strategic resource that is supported by related capabilities to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. The main principle is to obtain information superiority. Therefore, information

operations should be integrated and coordinated with a wide variety of core competencies.

Also included in the IO doctrine is recognition that the dynamic information environment must be assessed, collected, and analyzed. DoD directive S-3600.1, "Information Operations" (as revised) emphasizes the attainment of information superiority and the use of information age technologies to get the maximum strategic and tactical benefits for protection and situational awareness. The directive also mentions that all information that is obtained be integrated into operations to support engagement strategies and policies

Significant attention must be paid as to how information obtained in a foreign country must be handled. Two aspects deserve attention. One is how the information can be preserved and processed for evidential purposes, and the other is what can be legally secured by U.S. forces operating in a foreign country.

# Appendix C. Establishing a Chain of Custody

## What is a *chain of custody* and how can it be established?

The first goal of a direct action mission is to assure the safety of team members. An additional purpose, if electronic devices are discovered in the process of carrying out mission objectives, is to preserve the intelligence value of information contained on seized electronic devices and establish a chain of custody (if at all possible) of any seized electronic equipment, media, and materials.

The forensic analysts to whom custody of the seized items would be given need to know as much as they possibly can about the environment and circumstances under which the electronic media was seized. Critical to any successful legal proceedings in which the recovered electronic media is used would be a well-documented chain of custody. For example, a narcoterrorist's defense attorney could claim that seized electronic evidence was mishandled by a special operator or others, or suggest it was purposely manipulated to implicate the defendant. The concept of *reasonable doubt* might be introduced, and the guilty individual might otherwise be found innocent.

The operators should collect everything that can be legally obtained and document it. The marking and tagging of all equipment, media, and cables is necessary. Properly labeled cardboard boxes, if they are used for transport, are also necessary.

Document each item of seized equipment or media in an evidence log. An evidence log should contain the name of each item, time, date, and a description of any interactions that team members have with the item(s).

# Appendix D. Computer Forensics

## What is computer forensics?

*Computer forensics* actually begins when SOF operators scan, identify, document, and secure (SIDS) the digital assets to be seized and successfully secure them for transport, then eventually turn them over to forensic specialists and intelligence analysts for technical exploitation. The information that is gleaned can either be used for tactical or strategic intelligence as well as for legal purposes to prosecute enemy combatants, terrorists, and criminals.

At least one or more operators should be trained in basic computer forensic skills from scanning, identifying, documenting, and securing the enemy's digital assets. Any computer-based evidence is useless unless it is properly identified, collected, and preserved in a manner that follows the rules of admissibility so it can be used to successfully convict criminals or terrorists. The collection and presentation of computer evidence is, therefore, a technical matter that must nonetheless be undertaken in strict compliance with legal rules.

"Computer forensics involves the identification, extraction, documentation, preservation, and interpretation of computer data."[13] Electronic information that is seized as a result of special operations may be used for near-time intelligence-gathering purposes or as evidence in later legal proceedings, in which case chain of custody must be documented. Failure to provide for a well-documented chain of custody may destroy a court case against a criminal.

The collection and presentation of computer evidence is therefore a procedural and technical matter that must be undertaken in strict compliance with legal rules. An entry into an evidence log should be made that includes the time and date the media was recovered after the safety of the SOF team is assured.

## What are the potential forensic missteps?

All manipulation and handling of electronic devices or media should be documented to preserve the chain of custody and the authenticity of information. If the computer or device is to be unplugged, a quick determination

should be made as to whether the device is plugged into an uninterruptible power supply (UPS) or simply a wall socket. The computer should be unplugged from its source (from the wall if a UPS is absent). Otherwise, unplug the UPS from the wall socket. The computer (or device) will still run off of the reserve power supply for a short while (usually minutes). A determination may be made to keep the computer plugged into the UPS until the seized equipment can be plugged into a permanent power source.

Keep any seized electronic media away from electromagnetic fields (such as loudspeakers, magnets, motors, and radio transmitters). Secure the devices from all environmental extremes including heat, cold, dust, moisture, and severe vibrations or physical shocks.

Computers should be powered down only after pictures are taken of the monitors. Computers should never be turned off if a computer forensic specialist is available or the potential exists to keep the device powered (i.e., properly documenting the procedure and recharging laptop batteries).

## What are the general forensic procedures?

There are a number of general principles that underpin the *collection* and *assurance* of digital information seized during operations. The SIDS acronym captures the essence of what should be done by SOF.

The safety of personnel, first, is of paramount importance. All actions taken with regards to electronic information should avoid creating or causing changes or damage to electronic evidence. Personnel should have basic knowledge on how to preserve digital information. Appropriate tools should be used when possible. All steps taken to preserve digital intelligence collection should be fully documented including pictures or digital images and notes when possible. "Documentation of the scene should include the entire location—for example, the type, location, and position of computers, their components and peripheral equipment, and other electronic devices."[14]

Specific recommendations for conducting forensic computer operations in the *civilian* world follow:

a. Train personnel in basic computer forensic techniques.
b. Gather needed tools and a supply of packaging materials prior to the operation that will help to assure the safe removal of the digital devices and media (see Appendix F).
c. Prepare any preliminary paperwork (log sheets).

d. Brief personnel on any expected *digital evidence* or information that might be recovered.
e. Evaluate and train relative to the current legal considerations for targets and crime scenes.
f. Designate at least one forensic computer specialist.
g. Secure and perform initial assessment of the scene.
h. Identify computer and electronic devices and media.
i. Prevent any suspects found at the scene from interacting with the computer or other electronic devices or power supplies.
j. Avoid interacting with the computer or executing any programs.
k. Begin either an audio or written log to establish chain of custody.
l. Document computer and electronic evidence by labeling, photographing, or sketching.
m. Package all electronic devices, media. and other evidence for safe transport.
n. Label all parts and pieces and secure openings with evidence tape.
o. Remove and safely transport evidence and protect the physical integrity of the components.

# Appendix E. ASCII Table and Description

The Web site www.LookupTables.com provides a concise explanation of the ASCII code:

> ASCII stands for American Standard Code for Information Interchange. Because computers can only understand numbers, an ASCII code is the numerical representation of a character such as "a" or "@" or an action of some sort. ASCII was developed a long time ago and now the nonprinting characters are rarely used for their original purpose. The ASCII character table is shown below; it includes descriptions of the first 32 nonprinting characters. ASCII was actually designed for use with teletypes, thus the descriptions are somewhat obscure. If someone says they want your CV in ASCII format, what that means is "plain" text with no formatting such as tabs, bold, or underscoring—the raw format that any computer can understand. This request is usually so they can easily import the file into their own applications without issues. Notepad.exe creates ASCII text, or in Microsoft Word you can save a file as "text only."[16]

| Dec | Hx | Oct | Char | Dec | Hx | Oct | Html | Char | Dec | Hx | Oct | Html | Char | Dec | Hx | Oct | Html | Char |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 000 | Null | 32 | 20 | 040 |   | Space | 64 | 40 | 100 | @ | @ | 96 | 60 | 140 | ` | ` |
| 1 | 1 | 001 | Start of Heading | 33 | 21 | 041 | ! | ! | 65 | 41 | 101 | A | A | 97 | 61 | 141 | a | a |
| 2 | 2 | 002 | Start of Text | 34 | 22 | 042 | " | " | 66 | 42 | 102 | B | B | 98 | 62 | 142 | b | b |
| 3 | 3 | 003 | End of Text | 35 | 23 | 043 | # | # | 67 | 43 | 103 | C | C | 99 | 63 | 143 | c | c |
| 4 | 4 | 004 | End of Transmission | 36 | 24 | 044 | $ | $ | 68 | 44 | 104 | D | D | 100 | 64 | 144 | d | d |
| 5 | 5 | 005 | Enquiry | 37 | 25 | 045 | % | % | 69 | 45 | 105 | E | E | 101 | 65 | 145 | e | e |
| 6 | 6 | 006 | Acknowledge | 38 | 26 | 046 | & | & | 70 | 46 | 106 | F | F | 102 | 66 | 146 | f | f |
| 7 | 7 | 007 | Bell | 39 | 27 | 047 | ' | ' | 71 | 47 | 107 | G | G | 103 | 67 | 147 | g | g |
| 8 | 8 | 010 | Backspace | 40 | 28 | 050 | ( | ( | 72 | 48 | 110 | H | H | 104 | 68 | 150 | h | h |
| 9 | 9 | 011 | Horizontal Tab | 41 | 29 | 051 | ) | ) | 73 | 49 | 111 | I | I | 105 | 69 | 151 | i | i |
| 10 | A | 012 | New Line | 42 | 2A | 052 | * | * | 74 | 4A | 112 | J | J | 106 | 6A | 152 | j | j |
| 11 | B | 013 | Vertical Tab | 43 | 2B | 053 | + | + | 75 | 4B | 113 | K | K | 107 | 6B | 153 | k | k |
| 12 | C | 014 | New Page | 44 | 2C | 054 | , | ‘ | 76 | 4C | 114 | L | L | 108 | 6C | 154 | l | l |
| 13 | D | 015 | Carriage Return | 45 | 2D | 055 | - | - | 77 | 4D | 115 | M | M | 109 | 6D | 155 | m | m |
| 14 | E | 016 | Shift Out | 46 | 2E | 056 | . | . | 78 | 4E | 116 | N | N | 110 | 6E | 156 | n | n |
| 15 | F | 017 | Shift In | 47 | 2F | 057 | / | / | 79 | 4F | 117 | O | O | 111 | 6F | 157 | o | o |
| 16 | 10 | 020 | Data Link Escape | 48 | 30 | 060 | 0 | 0 | 80 | 50 | 120 | P | P | 112 | 70 | 160 | p | p |
| 17 | 11 | 021 | Device Control 1 | 49 | 31 | 061 | 1 | 1 | 81 | 51 | 121 | Q | Q | 113 | 71 | 161 | q | q |
| 18 | 12 | 022 | Device Control 2 | 50 | 32 | 062 | 2 | 2 | 82 | 52 | 122 | R | R | 114 | 72 | 162 | r | r |
| 19 | 13 | 023 | Device Control 3 | 51 | 33 | 063 | 3 | 3 | 83 | 53 | 123 | S | S | 115 | 73 | 163 | s | s |
| 20 | 14 | 024 | Device Control 4 | 52 | 34 | 064 | 4 | 4 | 84 | 54 | 124 | T | T | 116 | 74 | 164 | t | t |
| 21 | 15 | 025 | Negative Acknwledge | 53 | 35 | 065 | 5 | 5 | 85 | 55 | 125 | U | U | 117 | 75 | 165 | u | u |
| 22 | 16 | 026 | Synchronous Idle | 54 | 36 | 066 | 6 | 6 | 86 | 56 | 126 | V | V | 118 | 76 | 166 | v | v |
| 23 | 17 | 027 | End of Trans. Block | 55 | 37 | 067 | 7 | 7 | 87 | 57 | 127 | W | W | 119 | 77 | 167 | w | w |
| 24 | 18 | 030 | Cancel | 56 | 38 | 070 | 8 | 8 | 88 | 58 | 130 | X | X | 120 | 78 | 170 | x | x |
| 25 | 19 | 031 | End of Medium | 57 | 39 | 071 | 9 | 9 | 89 | 59 | 131 | Y | Y | 121 | 79 | 171 | y | y |
| 26 | 1A | 032 | Substitute | 58 | 3A | 072 | : | : | 90 | 5A | 132 | Z | Z | 122 | 7A | 172 | z | z |
| 27 | 1B | 033 | Escape | 59 | 3B | 073 | ; | ; | 91 | 5B | 133 | [ | [ | 123 | 7B | 173 | { | { |
| 28 | 1C | 034 | File Seperator | 60 | 3C | 074 | < | < | 92 | 5C | 134 | \ | \ | 124 | 7C | 174 | | | \| |
| 29 | 1D | 035 | Group Separator | 61 | 3D | 075 | = | = | 93 | 5D | 135 | ] | ] | 125 | 7D | 175 | } | } |
| 30 | 1E | 036 | Record Seperator | 62 | 3E | 076 | > | > | 94 | 5E | 136 | ^ | ^ | 126 | 7E | 176 | ~ | ~ |
| 31 | 1F | 037 | Unit Seperator | 63 | 3F | 077 | ? | ? | 95 | 5F | 137 | _ | _ | 127 | 7F | 177 | &#127; | Del |

# Appendix F. Equipment and Supplies for Information Operations

Among the equipment and supplies needed to secure a scene where electronic media is encountered would be a voice-activated audio recorder, a small digital camera, antistatic wrist band, evidence tape, labels, indelible writing pen, and antistatic wrapping materials or bags.

Digital cameras should be used to document the placement and condition of the area in which electronic devices and stored digital information are found. Pictures of the monitor screens, CDs, tapes, and recorders should be taken in their original location and secured in a dust- and shock-free environment.

Connections should be digitally documented and labeled for evidentiary purposes if time and personnel safety make it possible.

## What investigative tools should be used?

Special tools and resources should be used to obtain and secure electronic information. For initial securing, documentation, packaging, removal, and transporting, include the use of tamper-resistant evidence tape, flashlight, regular pliers, needle-nosed pliers, and rubber gloves.[15] Also include a handheld device that detects wireless signals.

Among the recommendations are antistatic packing materials that are sufficient size to package CPUs, PDAs, laptops, hard drives, and other media. Preprinted forms could be used to help ease the burden of maintaining a chain of custody after the seizure of evidence.

## How do you package and transport devices containing digital information?

Seized electronic devices should be placed in a hard shell carrying case that provides protection from dust, extremes in temperature, shock, and moisture.

All electronic devices that are seized must be documented, labeled, and packaged before they are transported. Doing so in the field might be very difficult to accomplish within a limited time without endangering the lives of personnel. Investigators should be mindful of any trace evidence (i.e.,

latent finger prints) and try to preserve it. Avoid using materials (i.e., like wool cloth) that could produce static electricity.

Avoid bending, folding, or scratching media such as storage disks, CDs, or DVDs. Properly label all containers in which seized material is to be transported.

# Endnotes


1. Dorothy Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, undated, from www.cs.georgetown.edu/~denning/infosec/nautilus.html, accessed 11 September 2000. Quoted in Randal A. Dragon, *Wielding the Cyber Sword: Exploiting the Power of Information Operations*, USAWC Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, 13 March 2001), 1.
2. Timothy E. Wright, "Field Guide Part One," The Field Guide for Investigating Computer Crime: Overview of a Methodology for the Application of Computer Forensics Part 1, www.securityfocus.com/infocus/1244, 3 (accessed June 2007).
3. Bernd Carsten Stahl, Moira Carroll-Mayer, and Peter Norris, "Forensic Computing: The Problem of Developing a Multidisciplinary University Course," in *Digital Crime and Forensic Science in Cyberspace*, ed. P. Kanellis, E. Kiountouzis, N. Kolokotronis, and D. Martakos (Hershey, PA.: The Idea Group, Inc., 2006), 295.
4. United States Secret Service, *Best Practices for Seizing Electronic Evidence* (U.S. Department of Homeland Security); www.forwardedge2.com/pdf/bestPractices.pdf (accessed June 2009), 3.
5. National Law Enforcement and Corrections Technology Center, Tech Beat, "Information Hide and Seek," a program of the National Institute of Justice; www.justnet.org/TechBeat%20Files/Hide_and_Seek.pdf (accessed June 2009), 1.
6. San Diego Regional Computer Forensics Laboratory, Guidelines for the Handling and Seizure of Digital Evidence; http://rcfl.org/downloads/documents/ERT_Brochure.pdf (accessed June 2009).
7. United States Secret Service, *Best Practices for Seizing Electronic Evidence*, 4.
8. Timothy E. Wright, "Field Guide Part One."
9 Bryan Pfaffenberger, *Webster's New World Dictionary of Computer Terms*, Eighth Edition (Foster City, CA: IDG Books Worldwide, Inc., 2000), 289.
10. Joint Publication 3-13, *Information Operations* (Washington, DC: Joint Chiefs of Staff, 13 February 2006), ix.
11. Ibid.
12. Ibid, xi.
13. Ibid, I-9
14. National Institute of Justice, electronic Crime Scene Investigation, *A Guide for First Responders, Second Edition*, NCJ 219941, April 2008, 19-20.
15. Timothy E. Wright, "Field Guide Part One."
16. "ASCII Codes," www.LookupTables.com (accessed 15 June 2009).


Joint Special Operations University
357 Tully Street
Alison Building
Hurlburt Field, FL 32544

https://jsoupublic.socom.mil